Amendments to the Specification:

Page 1, before line 3, the paragraph beginning with "The invention concerns" insert the following title and paragraph:

-- PRIORITY CLAIM

This is a U.S. national stage of PCT application No. PCT/FI00/00353, filed on April 25, 2000. Priority is claimed on patent application No. 990936 filed in Finland on April 26, 1999.--

Please replace the paragraph on page 1, line 11 with the following amended paragraph:

--Methods have been developed by means of which the receiver can notice[[, if]] whether somebody has altered the data between the sending end and the receiving end. The same methods can be used to detect[[,]] ~~if~~ whether the data has changed as a result of interference in the transmission path. Usually these methods utilize some kind of error detecting algorithm codes, like parity checking.--

Please replace the paragraph on page 2, line 15 with the following amended paragraph:

--Digital signature is used to identify the signer, who is the sender of the data. Advantageously, a secret and public key method is used in the digital signature ~~method it is used the secret and public key method~~ to achieve the signature for a certain data. Digital signature works for example like this: The sender of the message derives, for example, an error check value from the original message. After this the sender of the message encrypts the error check value with his secret key and sends the original message and the encrypted error check value to the receiver. The receiver decrypts the encrypted error check value with the sender's public key, which the sender has delivered to everybody. The receiver also derives the error check value

from the original message and compares these two error check values. If the values are equal, the message is from the correct sender. If they ~~don't~~ are not equal, the message has been corrupted.--

Please replace the paragraph beginning on page 2, line 27 with the following amended paragraph:

--It is planned that the mobile telecommunication networks, like the GSM, will be capable to transmit the data as ~~a~~ data packets. In GSM this is achieved by combining a so called GPRS (General Packet Radio Service) network to the GSM network. In figure 1 it is shown one possible arrangement of the GPRS network. There is shown a mobile station 101, which is in connection to MSC (Mobile Switching Centre) 104 through BTS (Base Transceiver Station) 102 and BSC (Base Station Controller) 103. There can be attached different types of networks, like for instance PSTN (Public Switched Telephone Network) network 105 and SS7 network 106[[,]] to the MSC 104. A new network element is arranged to the BSC 103, which is called PCU (Packet Control Unit) 107. However, it is by no means compulsory that the PCU (107) is located at the BSC (103), but it can be as a separate unit or attached to the BTS (102) as well. The PCU 107 is arranged to control the data packets. The packet network 112 is attached to other network topology through the PCU 107. Between the GPRS backbone network 113 and the PCU 107 it is arranged a SGSN (Serving GPRS Support Node) node 108. A GPRS register 109, or more generally a home location register that contains user related information, into which some kind of subscriber-related information concerning GPRS service network element is saved, is also a part of the GPRS network. GGSN (Gateway GPRS Support Node) nodes 110 are the elements through which any other kind of packet network 111, like IP, OSI data or X.25, can be attached to the GPRS network. In figure 1 the solid line symbolizes the data transmission and the signalling between the network elements and the broken line symbolizes that there are signalling

between the network elements. A similar arrangement is planned to the third generation mobile telecommunication networks for transmitting the data as ~~a~~ packet data.--

Please replace the paragraph beginning on page 4, line 10 with the following amended paragraph:

--The above stated objects are achieved by combining the authentication value ~~to~~ with the error check data so that ~~it does not add~~ the packet size is not increased. Combining the authentication value to error check data is done by using a logical function, for example. At the receiving end the combination of the error check value and the authentication value is processed so that the integrity of the data can be checked.--

Please replace the paragraph beginning on page 6, line 4 with the following amended paragraph:

--In the present invention the data transmitted is processed at the both ends, that is at the sending end and at the receiving end, in the same way so that the integrity of the message can be checked. At the sending end, as shown in figure 2, the error check value, which in this preferred embodiment is a CRC 205, is derived from the original data 201. Next, the authentication value 202, which can be derived for instance by using a packet number or a secret key as an input and a secret algorithm, is combined to the CRC field. The broken line describes that the authentication value 202 is in some way derived from the original data 201. The combination of the CRC 205 and the authentication value 202 is carried out in this preferred embodiment of the invention by using the logical function "exclusive-OR" (XOR) 203. XOR 203 is a function which produces an output of 1 when exactly one of its two inputs is 1. As a result, the data, which is to be sent, comprises the original data field 201 and another field, which consists of the

XORed value ~~308~~ 204 of the CRC 205 and the authentication value 202. To a man skilled in the art it is obvious that the authentication value 202 can be any value, which is advantageously possible to derive from the original data 201.--

Please replace the paragraph beginning on page 6, line 20 with the following amended paragraph:

--At the receiving end the data received is arranged to be processed vice versa, as shown in figure 3. The XORed data 308 is re-XORed 203 with the authentication value 302, which is the same as the authentication value 202 at the sending end in a case where the data sent is not changed. The authentication value 302 can be derived from the received data 301 in the same way as at the sending end. By using the rules of binary algebra the result of this re-XORing 203 is CRC value 304. By comparing 305 this CRC 304 to another CRC 303 calculated at the receiving end from the received data, it can be found, if the data has changed in the transmission path. If the comparison ~~302~~ 305 shows that the CRCs 303; 304 are the same, it means that the received data 301 has been transmitted without any changes 306. But, if the comparison 305 shows that the CRCs 303; 304 differ from each other, it means that the original data 201 has changed in the transmission path, or that the authentication value 302 was not correct at the receiving end. As a result, the data received can be erased ~~306~~ 307.--